MOTOROLA

BCA Interoperability Demonstration

Motorola NSM PKI

David Moyer
(410) 859-8319
David.Moyer@email.mot.com

8 September 1999

MOTOROLA

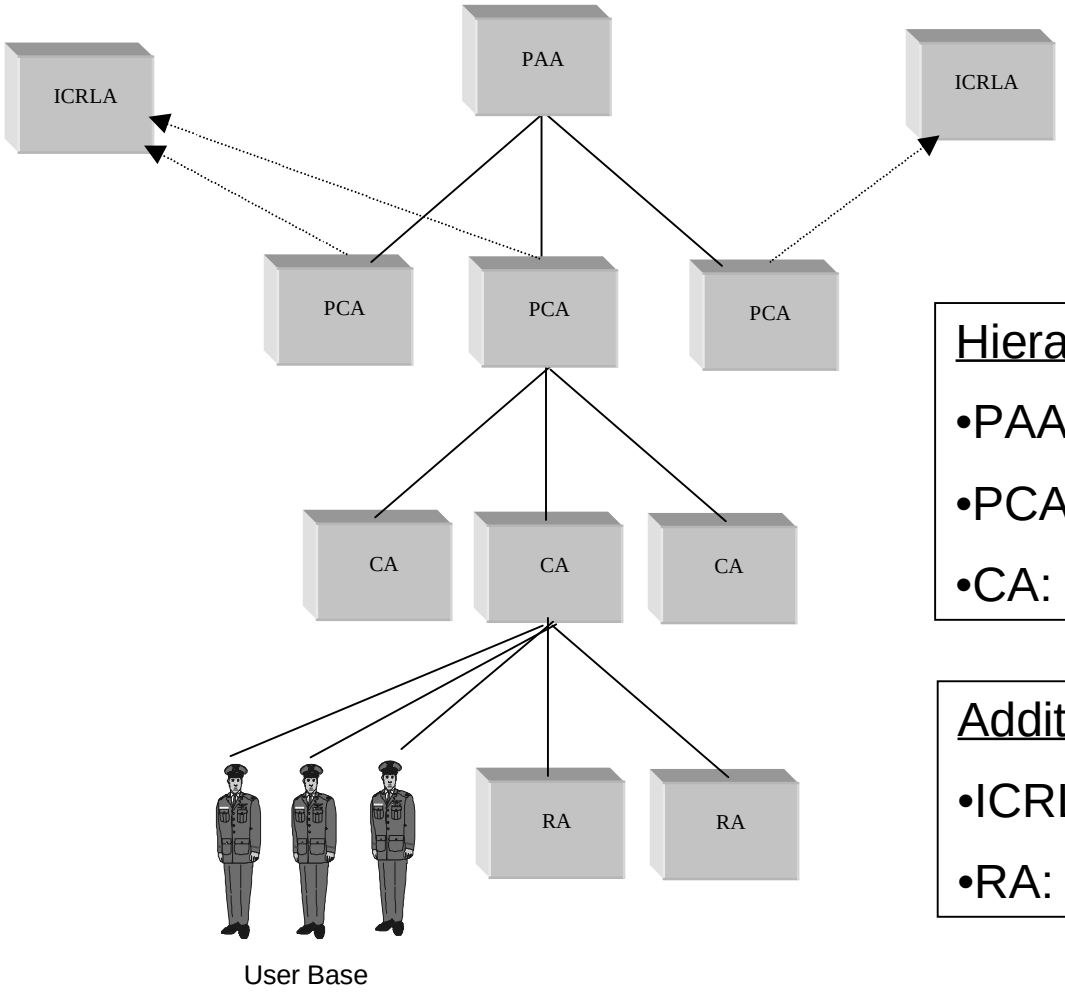
BCA Demonstration: Motorola Involvement

- Motorola is the current provider of the DoD High Assurance PKI: NSM
- This demonstration provides a unique opportunity to add useful capabilities to NSM and ring out issues in a test environment
- Provide an NSM hierarchy for the demonstration
- Investigate the technical, implementation, and policy issues associated with cross certifying the DoD high assurance PKI with the Bridge CA
- Add Cross Certification and RSA capability to the DoD High Assurance PKI to support the Bridge CA Cross Certification Demonstration

MOTOROLA

POC Name: David Moyer
Phone No. (410) 859-8319

Current Motorola NSM High Assurance PKI



Hierarchy includes 3 levels

- PAA: Policy Approving Authority
- PCA: Policy Creation Authority
- CA: Certification Authority

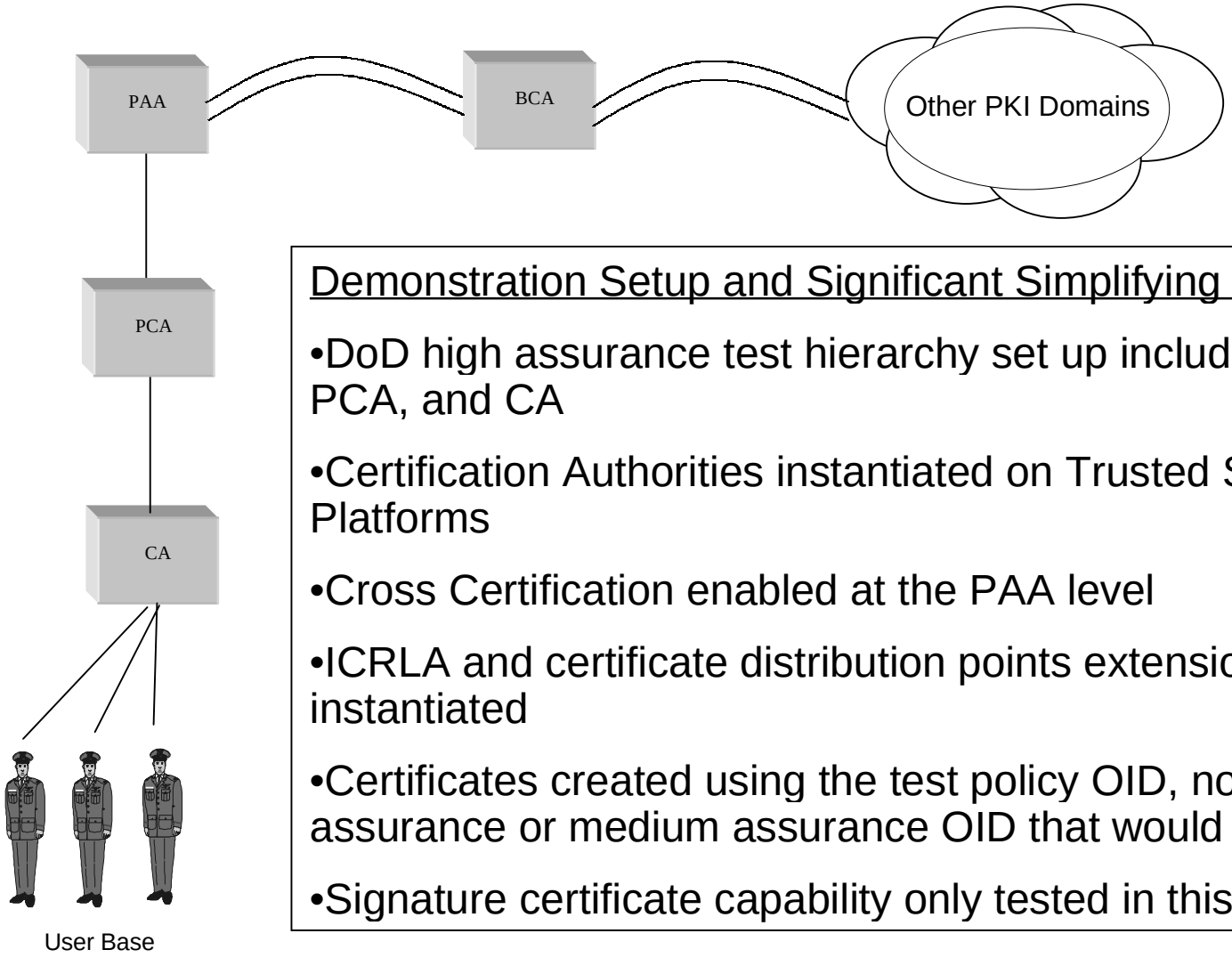
Additional Elements

- ICRLA: Indirect CRL Authority
- RA: Registration Authority

MOTOROLA

POC Name: David Moyer
Phone No. (410) 859-8319

Bridge CA Cross Certification Demonstration: NSM PKI Representation



Demonstration Setup and Significant Simplifying Assumptions

- DoD high assurance test hierarchy set up including a PAA, PCA, and CA
- Certification Authorities instantiated on Trusted Solaris Platforms
- Cross Certification enabled at the PAA level
- ICRLA and certificate distribution points extension not instantiated
- Certificates created using the test policy OID, not the high assurance or medium assurance OID that would be normal
- Signature certificate capability only tested in this demonstration

MOTOROLA

NSM Unique Features

- NSM developed for the DoD with some specific DoD unique requirements
- Primary user is the Defense Message System (DMS)
- High Assurance Software Security Architecture
  - Operating System: Trusted Solaris or SCO CMW+
  - Software Architecture separates trusted & untrusted processes
  - Software uses Trusted OS access control & role separation features
  - Design incorporated feedback from penetration testing of earlier MISSI CAWs
  - Robust Profiling & Penetration testing by NSA
- FORTEZZA (DSA, KEA, Skipjack) and LYNKS (added RSA) card supported
- Supports Multiple Algorithm Universal sets to enable domain separation
- CA CRLs are full and complete CRLs, additionally, CA revocation and CA/Subscriber compromise data sent to an ICRL Authority for more immediate compromise information dissemination

MOTOROLA

NSM Key Features

- **Extensible design capable of supporting:**
  - **Multiple algorithms (DSA, RSA, KEA)**
  - **Multiple security policies (DoD Class 3 and 4)**
  - **Subject Directory Attributes Extension used for access control and privilege information**
  - **Flexible security: Security Privilege Info Files (SPIF)**
- **Organizational Certificate Management**
  - **Supports 5 levels of traceability**
    - **From total traceability to hidden traceability to total anonymity**
  - **Management of shared encryption key certificates**
- **Multiple Directory Support**
  - **Can master certificates and CRLs on multiple Directories**
  - **Operates through the High Assurance Guard**

MOTOROLA

POC Name: David Moyer
Phone No. (410) 859-8319

NSM Infrastructure Summary